Packages - Bug #2931

[parabola-hackers]: keys are "unknown trust" after expiry/renewal

2020-11-15 07:44 PM - bill-auger

Status:	fixed	**% Done:**	0%
Priority:	bug		
Assignee:	bill-auger		
Category:			

Description

this is a recurring problem which happens whenever a signing key is expired and renewed; such that pacman rejects packages signed by that key - the files are unmodified since being published; and the report indicates successful verification

the problem persists after the signing key is renewed, and the keyring package is rebuilt - it is not obvious why, nor which software/interactions are involved, eg: the keyring package or its build process, the packaging metadata, or some interaction between pacman/gpg

we have tried removing the expired key from the keyring (the normal way, per hackers.git), then re-adding it; but that did not help - the next step down that path is to delete the entire hackers.git YAML file - IIRC the previous experiment, only the key entry was deleted

most of the experiments have been focussed on the keyring package build process - lately, i am looking toward other explanations

the current solution is to rebuild all afected packages from source - some experiments to try:
- simply replace the signatures with new ones
- run librerelease on the packages again
- rebuild the keyring with the signing key specified in hackers.git, instead of, or in addition to, the master key

my current theory, is that perhaps this is all expected behavior, and pacman-key is doing the thing right, but doing the wrong thing, by considering (intentionally or not) valid signatures from a presently expired key to be unacceptable - that is presumably due to the gpg exit status, although the program reports that it is a "good signature" - however that still would not explain why the warning /rejection persists after the key is renewed then the keyring package is rebuilt

pacman-key should consider the "good signature" per gpg to be of greater significance than the expiry date, and sufficient for package signature verification, unless the key was revoked - the expiry notice is a less significant than a warning, indicating no problem with the primary functionality in question: verifying the integrity/authenticity of a file/signature pair - if it were an invalid signature, or any error condition at all, i would expect: "Note:", would be rather like "Warning:", "Important!:", "Error:", etc

worse though, pacman indicates to the user, that the key has "unknown trust", which is misleading - it has exactly the same trust as before the expiry date, because nothing has changed - gpg is not reporting any error, and is not indicating any fault with the package verification - it is entirely a web-of-trust concern

it is a friendly reminder to the user, to contact this person, asking for that signature to be renewed, if the file in question is still valuable - if that person does not respond, nor extend the expiry, only then would it have a potential to become problematic - again, purely a web-of-trust or team management problem though - the package will always be faithfully verifiable just as the day it was published

Related issues:

Related to Packages - Bug #2146: [systemd]: error: signature from bill-auger ...	**fixed**
Related to Packages - Bug #2390: [bbswitch] pgp fail - blocks linux-libre upg...	**fixed**
Related to Packages - Bug #2572: [musescore] the current package has been sig...	**not-a-bug**
Related to Packages - Bug #2834: [cups-filters][tokyocabinet]: Signature is u...	**fixed**
Related to Packages - Housekeeping #2925: signature from bill-auger is unknow...	**fixed**
Related to Packages - Bug #2933: [icedove] bill-auger signature is possibly o...	**fixed**
Related to Packages - Bug #1527: [archlinux32-keyring] invalid signature	**duplicate**
Related to Packages - Bug #1344: PGP marginal trust in your-freedom, your-pri...	**fixed**

History

#1 - 2020-11-15 08:30 PM - bill-auger

- Related to Bug #2146: [systemd]: error: signature from bill-auger is unknown trust added

#2 - 2020-11-15 08:30 PM - bill-auger

- Related to Bug #2390: [bbswitch] pgp fail - blocks linux-libre upgrade added

#3 - 2020-11-15 08:30 PM - bill-auger

- Related to Bug #2572: [musescore] the current package has been signed by an invalid PGP signature added

#4 - 2020-11-15 08:30 PM - bill-auger

- Related to Bug #2834: [cups-filters][tokyocabinet]: Signature is unkown trust added

#5 - 2020-11-15 08:30 PM - bill-auger

- Related to Housekeeping #2925: signature from bill-auger is unknown trust added

#6 - 2020-11-15 08:53 PM - bill-auger

- Description updated

#7 - 2020-11-17 07:03 AM - bill-auger

- Description updated

- Subject changed from [parabola-hackers]: keys are "unknown trust" after expiry/renweal to [parabola-hackers]: keys are "unknown trust" after expiry/renewal

#8 - 2020-11-21 02:49 AM - bill-auger

- Related to deleted (Housekeeping #2925: signature from bill-auger is unknown trust)

#9 - 2020-11-21 02:54 AM - bill-auger

specifying the signing sub-key in hackers.git, instead of the master key, has fixed the problem, at least temporarily - my signing key is set to expire again today, so we should know soon if that is a permanent solution

#10 - 2020-11-21 04:34 AM - bill-auger

- Related to Housekeeping #2925: signature from bill-auger is unknown trust added

#11 - 2020-11-21 04:35 AM - bill-auger

- Related to Bug #2933: [icedove] bill-auger signature is possibly outdated added

#12 - 2020-11-23 12:38 AM - GNUtoo

- Related to Bug #2936: librestage not working with pacman-mirrorlist added

#13 - 2020-11-23 12:41 AM - GNUtoo

> the current solution is to rebuild all affected packages from source [...]

I've been trying to do that but I'm stuck due to bug #2936

AFAIK we don't have many packages to rebuild to enable the creation of a librechroot:

- filesystem -> done for x86_64
- pacman-mirrorlist -> fails
- linux-libre-api-headers -> done for x86_64

Then it might unbreak the ability to rebuild more and more packages as needed without workarounds (which are more time consuming if you don't want any nasty side effects).

#14 - 2020-11-23 04:24 PM - bill-auger

the problem appears to be fixed now - i deduce that the root of the problem is in the pacman install hook on the local machine, when pacman assigns "trust-level' to the keys - though the way pacman handles this could be improved, i think we can chalk this one up to user error, and strictly-speaking: not a bug

apparently, the master key can be trusted, while any of the subkeys are not necessarily trusted; and pacman only trusts the one specified key, ignoring subkeys if the master key was specified, and ignoring the master key if a subkey was specified - so the solution appears to be: to specify the signing key in hackers.git - if that is a subkey, it forces pacman to explicitly trust the subkey

then again, i did not ever have the same problem as oaken-source's key; and i dont know if oaken-source signs packages with a subkey - we should verify that any of oaken-source's packages which may still be in the system are installable now, and/or if oaken-source can publish packages now

the pacman eerror mesage "unknown trust" is extremely misleading in this case; because the key specified in hackers.git *is* trusted during install - ideally, an error would be thrown during the install of the keyring package, (or better yet, during the package build), rather than the current behavior of defering the error condition until pacman attempts to verify some other package - unfortunately, pacman can not know if the key being signed (or any of it's subkeys) will actually be used to sign packages - in theory, it could detect if any of the subkeys of that key have been used in the past to sign packages already in the system, and insist on verifying and assigning a trust-level to those also; but that could be an expensive operation

#15 - 2020-11-30 11:04 AM - bill-auger

- Related to deleted (Bug #2936: librestage not working with pacman-mirrorlist)

#16 - 2020-11-30 11:04 AM - bill-auger

- Assignee set to bill-auger

#17 - 2020-11-30 11:04 AM - bill-auger

- Status changed from in progress to fixed

#18 - 2021-04-09 04:36 PM - bill-auger

as an update, this latest keyring rebuild (probably) verified that the fix was correct (put the signing key in hackers.git, not the master key)

i let my key expire again (in the keyring) before rebuilding the keyring - the key was not actually expired at any time though; so it is not a complete verification of correctness - its not obvious that it would make any difference; but who knows

#19 - 2021-05-14 01:54 PM - bill-auger

- Related to Bug #1527: [archlinux32-keyring] invalid signature added

#20 - 2021-05-14 02:16 PM - bill-auger

- Related to Bug #1344: PGP marginal trust in your-freedom, your-privacy and parabola-keyring added

#21 - 2022-09-24 11:09 AM - bill-auger

as an update, the previous "fix" (put the signing key in hackers.git, not the master key) was not sufficient; but i believe that i have finally cracked it

it happened again with my key and oaken-source's key; so i had to dig into it again - this fix has worked for everyone so far, and is now in the published 'pacman' package

https://git.parabola.nu/abslibre.git/tree/libre/pacman/9002-pacman-key-updatedb.patch

the diagnosis appear to be this: that `gpg --check-trustdb` command runs on every keyring install/upgrade, per '.install' hooks; but normally it does nothing - gpg decides if the update should actually be performed based on a schedule - the trick is to force it to always update (with `--yes`) - i expect that no one will have this same old problem again

its not perfect - ive noticed the update command (sometimes?) runs twice (which is harmless); but maybe it could be improved (given some time to make sure it really is a satisfying fix)